CLAIMS

This listing of claims will replace all prior version and listings of claims in the application:

1. (Currently amended) A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious ~~intrusion~~ activity, comprising the steps of:

monitoring packets exchanged between two hosts on the data communication network;

identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined characteristic ~~assigning packets to a flow~~;

~~collecting flow data from packet headers;~~

assigning ~~analyzing collected flow data to assign~~ a concern index value to an identified ~~the~~ flow based upon a ~~probability~~ predetermined characteristic of ~~that~~ the flow ~~was not normal for data communications~~;

maintaining an accumulated concern index comprising concern index values for one or more identified ~~from~~ flows associated with a host; and

issuing an alarm signal ~~once~~ in the event that the accumulated concern index ~~has exceeded~~ for a host exceeds an alarm threshold value.

2. (Currently amended) The method of claim 1, wherein the predetermined characteristic of a flow is selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet ~~the flow consists of the packets exchanged between two hosts that are associated with a single service~~.

3. (Currently amended) The method of claim 1, further comprising the step of communicating a message to a firewall to drop packets going to or from the particular host in response to ~~wherein~~ the alarm signal ~~updates a firewall for filtering packets transmitted by a host~~.

4. (Currently amended) The method of claim 1, wherein the alarm signal generates a notification to a ~~the~~ network administrator.

5. (Currently amended) The method of claim 1, wherein each concern index value associated with a predetermined event ~~respective potential intrusion activity~~ is a predetermined fixed value.

6. (Currently amended) A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious ~~intrusion~~ activity, comprising the steps of:

monitoring packets exchanged between two hosts that are associated with a single service on the data communications network;

identifying a flow corresponding to a predetermined plurality of ~~assigning packets to a flow, wherein a flow consists of the~~ packets exchanged between the two hosts ~~that are associated with a single service~~;

collecting flow data from packet headers of the packets in the identified flow;

based on the collected flow data, assigning ~~analyzing collected flow data to assign~~ a concern index value to the flow based on a predetermined characteristic of the flow ~~wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value~~;

maintaining an accumulated concern index from flows that are associated with a particular host; ~~and~~

issuing an alarm signal in the event that ~~once~~ the accumulated concern index for the particular host exceeds ~~has exceeded~~ an alarm threshold value; and

in response to the alarm signal, sending a message to a utilization component.

7. (New) (NOTE: NO CLAIM PRESENTED FOR CLAIM 7 IN ORIGINAL APPLICATION DUE TO TYPOGRAPHICAL ERROR) The method of claim 6, wherein the utilization component is selected from the group comprising: network security device, email, SNMP trap message, beeper, cellphone, firewall, network monitor, user interface display to an operator.

8. (Currently amended) A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious ~~intrusion~~ activity, comprising the steps of:

monitoring the exchange of packets between two hosts each having a particular Internet Protocol (IP) address;

identifying a flow corresponding to a predetermined plurality of packets exchanged between a particular port of one of the hosts that remains constant during the plurality of packets ~~assigning packets to a flow, wherein a flow consists of the packets exchanged between two Internet Protocol addresses with at least one port remains constant~~;

collecting flow data from packet headers of the packets in the identified flow;

based on the collected flow data, assigning ~~analyzing collected flow data to assign~~ a concern index value to the flow;

maintaining a host data structure containing ~~an~~ accumulated concern index values from a plurality of flows that are associated with the particular host; and

issuing an alarm in the event that ~~once~~ the accumulated concern index values for the particular host has exceeded an alarm threshold value.

9. (Currently amended) The method of claim 8, wherein each concern index value associated with a respective potential suspicious ~~intrusion~~ activity is a predetermined fixed value.

10. (Currently amended) A system for analyzing network communication traffic and determining potential suspicious activity, comprising:

~~a computer system operable to classify packets into flows, collect flow data from packet header information, analyze collected flow data to assign a concern index value wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value, and generate an alarm signal;~~

a computer system operative to:

a) monitor the communication of packets on a data communication network;

b) classify the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;

c) analyze the flows in order to assign a concern index value to a flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;

d) generate an alarm signal in response to cumulated concern index values; and a communication system coupled to the computer system operative to receive packets communicated between hosts on the network ~~operable to send packets from one host to another host~~.

11. (Currently amended) A system for analyzing network communication traffic and determining potential suspicious activity, comprising:

~~a processor operable to classify packets into flows, collect flow data from packet header information, analyze collected flow data to assign a concern index value wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value, and generate an alarm signal;~~

a processor operative to:

a) monitor the communication of packets on a data communication network;

b) classify the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;

c) maintain a flow data structure for storing data corresponding to a plurality of flows;

d) analyze the flows in the flow data structure in order to assign a concern index value to a flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;

e) cumulate assigned concern index values of one or more flows associated with a particular host;

f) maintain a host data structure for storing data associating a cumulated concern index value with each one of a plurality of hosts; and

g) generate an alarm signal in response to cumulated concern index values in the host data structure;

a memory coupled to the processor and operative ~~operable~~ to store the flow data structure and the host data structure ~~the flow data~~;

~~a database coupled to processor operable to store log files~~; and

a network interface coupled to the processor operative to receive packets on the data communication network ~~operable to monitor network traffic~~.

12. (Currently amended) A method of analyzing network communication traffic on a data communication network for potential suspicious ~~intrusion~~ activity, comprising the steps of:

monitoring packets exchanged between two hosts on the data communication network;

~~analyzing packet header information;~~

identifying packets provided by one of the two hosts that have ~~determining~~ a transport level protocol specifying a packet format that includes a data segment ~~of a data area~~;

in response to determination that the transport level protocol is a User Datagram Protocol (UDP) packet and the data segment associated with the UDP packet contains two bytes or less of data, storing a concern index value of a predetermined amount in a memory in association with information identifying the host that issued the UDP packet; and

issuing an alarm when the cumulated concern index value associated with the host exceeds a predetermined threshold level ~~transport level protocol is identified as User Datagram Protocol (UDP) and the data~~

~~segment associated with User Datagram Protocol packet contains two or less bytes of data~~.

13. (New) The method of claim 6, wherein a flow is characterized by a predetermined characteristic selected from the group comprising: the elapse of predetermined period of time where no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

14. (New) The method of claim 8, wherein a flow is characterized by a predetermined characteristic selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

15. (New) The system of claim 10, wherein a flow is characterized by a predetermined characteristic selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

16. (New) The system of claim 11, wherein a flow is characterized by a predetermined characteristic selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

17. (New) The method of claim 1, wherein the single service comprises a port number remaining constant for a plurality of packets.

18. (New) The method of claim 1, wherein the suspicious activity is from an inside address or from an outside address.

19. (New) The method of claim 1, wherein the concern index for a suspicious activity is derived by reference to a table of predetermined suspicious activities each having a predetermined concern index value.

20. (New) The method of claim 1, wherein the host for which the concern index is accumulated is an inside host.

21. (New) The method of claim 1, wherein the host for which the concern index is accumulated is an outside host.

22. (New) The method of claim 1, wherein the steps are carried out in a monitoring appliance.

23. (New) The method of claim 22, wherein the monitoring appliance is installed behind a firewall.

24. (New) The method of claim 22, wherein the monitoring appliance is connected before a firewall.

25. (New) The method of claim 22, wherein the monitoring appliance is connected in a DMZ.

26. (New) The method of claim 22, wherein the monitoring appliance is configured to operate as a pass-by filter.

27. (New) The method of claim 22, wherein the monitoring appliance is coupled to a network device.

28. (New) The method of claim 27, wherein the network device is selected from group comprising: router, switch, hub, tap.

29. (New) The method of claim 27, wherein the network device is a network security device.

30. (New) The method of claim 1, wherein the monitoring of packets comprises monitoring on packet header information only.

31. (New) The method of claim 1, wherein the monitoring of packets is carried out in a device operating in a promiscuous mode.

32. (New) The method of claim 1, wherein the alarm signal is provided to a utilization component.

33. (New) The method of claim 32, wherein the utilization component is selected from the group comprising: network security device, email, SNMP trap message, beeper, cellphone, firewall, network monitor, user interface display to an operator.

RECORD OF INTERVIEW

The applicants would like to thank Examiner Ronald Baum for his helpful comments and suggestions during the telephone interview with the undersigned and associate attorney Wendell Peete on December 14, 2005. During the telephone interview certain aspects of novelty over the cited art were discussed.

Pursuant to 37 C.F.R. § 1.133(b), the following description is submitted as a complete written statement of the reasons presented at the interview as warranting favorable action. The following statement is intended to comply with the requirements of MPEP § 713.04 and expressly sets forth: (A) a brief description of the nature any exhibit shown or any demonstration conducted; (B) identification of the claims discussed; (C) identification of specific prior art discussed; (D) identification of the principal proposed amendments of a substantive nature discussed; (E) the general thrust of the principal arguments; and (F) a general indication of any other pertinent matters; and (G) the general results or outcome of the interview, if appropriate.

(A) No exhibits were shown or discussed.

(B) The independent claims were discussed, in particular certain aspects relating to <u>flow-based</u> detection of network intrusions.

(C) The *Shipley* (6,119,236) patent was discussed.

(D) No proposed amendments were officially presented or discussed, but the claim amendments presented in this paper are consistent with the discussion.

(E) The general thrust of the discussion was as set forth below in the next paragraphs.

(F) No other matters were discussed.

(G) No agreement was reached during the interview regarding the claims.

The general thrust of the discussion was that the *Shipley* patent did not disclose, teach, or suggest the claimed aspects of a <u>flow-based</u> detection of suspicious network activity such as intrusions. As discussed, and among other aspects, the claimed invention(s) provide for detection of suspicious network activity based on the monitoring of packets between two hosts on a network that are associated with a single service, and characterizing a group of such packets as a "flow."

The examiner suggested that the claims be amended to more particularly specify what a flow is and how the flows are used to determine the recited "concern index." No agreement on particular claim language was reached, pending submission of a formal amendment.

The amendments herein and comments that follow are intended to be consistent with the remarks made during the interview.

Further, for the record, on or about February 1, 2006, the undersigned had a subsequent telephone conference with the examiner to discuss the submission of a replacement (or supplemental, or substitute) amendment so as to clarify certain language relating to identifying a flow based on "predetermined characteristics" as opposed to "delimited by a predetermined event," the latter of which is believed to be unduly narrow. The examiner suggested filing a substitute or supplemental response. This paper is in response to that discussion.

In the event that the foregoing record is not considered complete and accurate, the Examiner is respectfully requested to bring any incompleteness or inaccuracy to the attention of the undersigned.